IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA	]	
	]	
v.	]	No. 23-cr-118-SE-AJ-01
	]	
TYLER ANDERSON	]	

REPLY TO GOVERNMENT'S OBJECTION TO MOTION TO SUPPRESS AND ADDITIONAL ARGUMENT

Tyler Anderson respectfully submits his Reply to the Government's Objection to his Motion to Suppress Evidence and additional arguments. Anderson responds by asserting that: (1) the search of the phone required explicit warrant authorization; (2) the warrant failed the particularity requirement; (3) obtaining the passcode and searching the phone was beyond the scope of what the search warrant authorized and thus are fruits of an unlawful search; (4) *United States v. Patane*, 542 U.S. 630 (2004)(Thomas, J., plurality) requires the exclusion of the physical fruits of a coerced statements; (5) *Patane*'s rule of excluding only physical objects should not be extended to digital devices. Grounds follow:

I. The search of Anderson's phone required explicit warrant authorization.

Searching a cell phone "would typically expose to the government far more than the most exhaustive search of the house…contain[ing] in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Riley v. California*, 573 U.S. 373, 396–97 (2014). To protect these privacy interests, searching a phone generally requires a warrant, including where defendants enjoy diminished expectations of privacy, such as incident to an arrest. *See id* at 401.

Such a requirement is "not merely an inconvenience to be somehow weighed against the claims of police efficiency," but are "an important working part of our machinery of

government." *Id*. Even where probable cause a supports an inference that a phone contains evidentiary value, law enforcement may seize the phone but must obtain a warrant before examining its contents. *See United States v. Henry*, 827 F.3d 16, 28 (1st Cir. 2016). Here, where Agent Howe stated that there was probable cause to believe that Anderson used a cell phone associated with 603-xxx-8914 to violate 18 U.S.C. § 875(c), then searching the phone required a warrant.

II. The warrant failed to meet the Fourth Amendment's particularity requirement.

"The Fourth Amendment prohibits the issuance of any warrant except one 'particularly describing the place to be searched, and the persons or things seized.'" *United States v. Rogers*, 521 F.3d 5, 9 (1st Cir. 2008) (quoting U.S. Const. amend IV). "Any search intruding upon [an individual's] privacy interest must be justified by probable cause and must satisfy the particularity requirement, which limits the scope and intensity of the search." *Rogers*, at 9 (quoting *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986)). A sufficiently particular warrant (1) provides "enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) [is not] too broad in the sense that it includes items that should not be seized." *United States v. Lindsey*, 3 F.4th 32, 40 (1st Cir. 2021).

In the digital context, courts have "invalidated warrants authorizing computer searches 'where [they] could discern no limiting principle: where, for example, the warrant permitted a search of 'any and all information, data, devices, programs, and other materials,' or 'all computer and non-computer equipment and written materials in [a defendant's] house.'" *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017). Focusing the warrant on evidence of "specific federal crimes or to specific types of material" also provides sufficient particularity. *Id* at 1245. Given that cell phones are "'minicomputers that also happen to have the capacity to be used as a

telephone,'" the requirement of a limiting principle extends to phone searches. *Id*. at 1245, quoting *Riley*, 134 S.Ct. at 2489. In evaluating the particularity of search warrants targeting cell phones, courts may consider whether the warrant specified the "material (e.g., text messages, photos, or call logs) to be seized. *Id*.

No limiting principle existed in the warrant to guide and control the execution of the search and seizure. By the time Agent Howe applied for the warrant, his investigation had developed probable cause to seek text messages sent on December 8, 2023, in relation to alleged violations of 18 U.S.C. § 875(c). Yet the resultant warrant authorized the seizure of potential evidence without any temporal or material limitation; the warrant targeted neither text messages evidencing a violation of 18 U.S.C. § 875(c) nor communications dated December 8, 2023. This is similar to *Russian*, where the court held that a warrant was insufficiently particularized to authorize the search of the defendant's cell phones because the warrant only permitted a search of the defendant's residence and seizure of any cell phones found inside without specifying that officers could seize text messages. *See* 848 F.3d at 1245.

Furthermore, this is unlike *United States v. Palms*, where the defendant unsuccessfully challenged the particularity of a warrant, as well as argued that the searched exceeded the warrant's scope. 21 F.4th 689, 694-95 (10th Cir. 2021). There, police arrested the defendant, seized his cell phone, and obtained a warrant specifically authorizing a search of the phone for evidence including, but not limited to SMS (short message service) and MMS (multimedia message service). *Palms*, 21 F.4th at 694. The court concluded that the warrant provided a sufficiently particular search authorization. *See id*. at 700. Here, the warrant did not focus the investigation to electronic data contained in the contents of Anderson's cell phone, including SMS or related digital communications.

The present warrant is also unlike *Corleto*, where police executed a warrant to search the defendant's vehicles and residence for "records and visual depictions of minors engaged in sexually explicit conduct" and to seize "[a]ny computer or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including the production, receipt, possession, distribution, or transportation of child pornography." *United States v. Corleto*, 56 F.4th 169, 173, 177 (1st Cir. 2022). The court found the *Corleto* warrant sufficiently particular because, "[i]n light of the evidence reported in the affidavit concerning the nature of the offense, the seizure and subsequent search of all such devices in the [defendant's] residence and vehicles 'was about the narrowest definable search and seizure reasonably likely to obtain the images.'" *Id*. at 177.

In contrast, the present warrant failed to properly narrow the seizure authorization; rather than allow police to search for and seize text messages allegedly sent on December 8, 2023, the warrant permitted police to seize "all evidence, contraband, or property designed for use, intended for use, or used relating to violations" of the threat statute, "records and information relating to" threats and the 603- xxx-8914 phone number, and correspondence and instant messaging logs amount to evidence of who owned, used, or controlled Anderson's mobile phone. ECF Doc. 21-1 at 4, 7. Such breadth provided law enforcement officers with "unbridled discretion to rummage at will among [] [Anderson's] private effects" within his cell phone and, thus, the warrant failed to meet the Fourth Amendment's particularity requirement. *United States v. Wurie*, 728 F.3d 1, 14 (1st Cir. 2013), aff'd sub nom. *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014).

III. The search of Anderson's phone exceeded the scope of the warrant.

If the scope of a search exceeds what is permitted by a validly issued search warrant, the

search and any subsequent seizure are unconstitutional. *Horton v. California*, 496 U.S. 128, 140 (1990). Here, the warrant did not authorize law enforcement officers to search Anderson's phone. Attachment A of the warrant permitted the *search* of only Anderson's person and his residence at 245 Central Avenue, #1, Dover, New Hampshire. ECF Doc. 21-1 at 1. (*emphasis added*). Attachment B allowed the *seizure* of Anderson's Samsung Galaxy S10E, as well as the "passwords…necessary to access" it. ECF Doc. 21-1 at 4 (attach. B ¶1(a), 2(i)) (*emphasis added*). Any contention that the warrant might have authorized a search of the contents within Anderson's phone must instead rely upon three separate provisions within Attachment B,: (1) permission to seize "records and information relating to threats to injure the person of another," and (2) "chat," correspondence, and instant message logs evidencing who used, owned, or controlled a computer responsive to the warrant, as well as (3) the authority to review electronic storage media and electronically stored information seized or copied pursuant to the warrant for the purpose of locating additional evidence. ECF Doc. 21-1 at 4, 7.

However, searching the contents of Anderson's phone falls beyond the scope of these three authorizations. First, permission to seize "records and information relating to threats to injure the person of another" does not amount to authority to search Anderson's phone. The warrant broadly defines "computer" as including "mobile phones." ECF Doc. 21-1 at 7. Separately, the warrant describes "records" and "information" as including "all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form." ECF Doc. 21-1 at 6. That the warrant identifies "hard disks or other media that can store data" as illustrative examples of "computer or electronic storage" establishes that "records and information" pertain to any "form of computer"

storage, rather than "any form of computer," inclusive of a mobile phone. *Id*. Thus, the plain language of the warrant distinguishes Anderson's phone from the records and information to be seized. Despite the allegation of the affidavit supporting the warrant application that Anderson transmitted a threat via text message, the warrant itself neither mentions text messages nor implies that analogous digital communications constitute "records and information." ECF Doc. 21-1 at 4. To interpret "records and information" as including text messages cuts against the plain meaning of the term. The authority to seize hard disks or digital storage devices relating to the alleged threats (e.g., a CD-ROM labelled with PC1's name) did not enable officers to view the contents of Anderson's phone.

Second, permission to seize "chat," correspondence, and instant message logs did not extend to search Anderson's phone contents. If officers could seize a computer or storage medium holding records or information responsive to the warrant, then the warrant further authorized the seizure of evidence of who used, owned, or controlled that item "at the time the things in the warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,…chat, instant messaging logs[,]…and correspondence". ECF Doc. 21-1 at 4. Commonly understood, text messages do not constitute evidence of who used, owned, or controlled a cell phone at a given time, as they do not require their author to identify themselves. Moreover, given that the phone was locked when officers obtained it from Anderson's bed, nothing in plain view indicated that the phone contained chat, instant messaging logs, or correspondence that could identify the person who used, owned, or controlled the phone on December 8, 2023.

Third, the warrant's authorization for law enforcement agents to review "electronic storage media and electronically stored information" that is "seized or copied…in order to locate

evidence" and other material responsive to the warrant similarly does not constitute authorization to access and search Anderson's phone. ECF Doc. 21-1 at 7. As argued supra, Attachment B defines "information" as "all forms of creation or storage," including any form of computer storage or "electronic storage (such as hard disks or other media that can store data). The Attachment also defines "storage medium" as including "any physical object upon which computer data can be recorded…[including] hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optic data." *Id*. at 4. The warrant distinguishes these definitions pertaining to digital storage devices from that of "computer," which includes "mobile phones." ECF Doc. 21-1 at 7. Thus, the review authorization does not extend to Anderson's phone.

In summary, while Attachment A authorized the search of Anderson and his residence, Attachment B permitted only the seizure of his phone, his phone passcode, digital and analog records, evidence showing the ownership and use of certain devices (e.g., logs, correspondence, and instant messages), and the review of digital storage devices. To construe these seizure authorizations as permission to search the contents of Anderson's phone would contradict *Riley*, which characterized the cell phone as a greater locus of privacy interests than that of the home, and thus demanding a warrant for its search. *See Riley*, 573 U.S. at 396–97, 401.

Here, law enforcement officers viewed the contents of Anderson's phone, including folders containing undeleted and deleted text messages. When law enforcement officers did so, they exceeded the scope of their warrant. The search of Anderson's phone is unlike *Palms*, where the police properly executed a search warrant by "limit[ing] [their] search to the time-period when [the defendant] knew [the alleged victim] and viewed the types of files that were most likely to contain evidence of the crime of human trafficking." *United States v. Palms*, 21 F.4th 689, 701 (10th Cir. 2021). In executing the present warrant, the record indicates that

officers limited their search neither to the relevant timeframe nor to text messages. Thus, viewing the contents of Anderson's phone exceeded the scope of the warrant.

IV. Involuntary statements and evidence derived from those statements must be excluded at trial.

Determining whether a confession is voluntary, a court assesses whether "the will of the defendant ha[s] been overborne so that the statement was not his free and voluntary act." *United States v. Jacque*s, 744 F.3d 804, 809 (1st Cir. 2014). The Court considers "the totality of the circumstances, including both the nature of the defendant's activities and the defendant's situation." *Id*. This analysis takes into account the "length and nature of the questioning, promises or threats made by investigators, [ ] deprivation of the suspect's essential needs" and "the defendant's personal circumstances, including his age, education, intelligence, [ ] mental condition, as well as his prior experience with the criminal justice system." *Id*.

Here, the totality of the circumstances weighs in favor of finding Anderson's statements involuntary. Prior to the forced entry into Anderson's home, law enforcement knew of Anderson's history of mental health issues. Based on additional discovery, counsel learned that on December 8, 2023, law enforcement conducted a search of their database and cross-agency databases and learned that Anderson was listed in a Salem, NH database as "Suicidal" and in another listing as involved in an involuntary emergency admission. The database also showed that Anderson had no prior arrest history. Despite knowing of Anderson's vulnerabilities, multiple armed law enforcement officers and agents forcibly entered Anderson's home, handcuffed, and questioned him. They did so without first advising him of his *Miranda* rights, without asking him about his mental health condition, or inquiring about any mental health medication. *Cf. United States v. Hughes*, 640 F.3d 428, 440 (1st Cir. 2011)("Police officers must, of course, be sensitive to a suspect's mental condition. They must exercise caution when

dealing with a suspect whose compromised mental state is known to them."). Although law enforcement's use of trickery does not automatically render a confession coerced, "some aggravated types of police chicanery can render a confession involuntary." *Id.* at 439 (*citing Lynumm v. Illinois*, 372 U.S. 528, 534 (1963)). Although the government contends that law enforcement did not subject Anderson to trickery, an agent told Anderson that providing the passcode would make the process easier and possibly prevent damage to his phone. This statement was made despite the government's assertion that law enforcement had the tools and ability to access the data on Anderson's phone without using his passcode. ECF Doc. 21 at 8.

V. If the Court finds the statements were voluntarily made, *Patane* should not be applied to the contents of a digital device.

While assuming the digital passcode was an excludable statement, the government asserts that only the statement itself – the act of the defendant providing the passcode – should be suppressed. ECF Doc. 21 at 5 (*citing United States v. Patane*, 542 U.S. 630, 642-43 (2004)(Thomas, J., plurality) *id*. at 644-45 (Kennedy, J., concurring in judgment). In *Patane,* the defendant made an *unMirandized* statement about possessing a firearm. *Id*. at 635. The police then located the firearm in Patane's bedroom and seized it. *Id*. While the Fifth Amendment warranted the suppression of the self-incriminating statement, the plurality ruled that physical fruits of an uncoerced statement obtained in violation of *Miranda* need not be suppressed. *Id*. at 639-40. Accordingly, Patane's *unMirandized* statement concerning the location of the gun would be suppressed, but the gun (the object) would be admissible. *Id.*

The physical object (a gun) deemed admissible in *Patane* is fundamentally different from evidence found on digital phones. Accordingly, this Court should find *Patane* inapplicable to the facts of this case. *See generally* Abbey Flynn, Physical Fruits vs. Digital Fruits: Why Patane

Should Not Apply to the Contents of Digital Devices, 2021 U.Ill. J.L. Tech. & Pol'y 1 (2021) (arguing *Patane* should not apply to contents of digital devices and articulating deterrence value). Courts have recognized the inextricable connection of protections afforded by the Fifth and Fourth Amendments when addressing digital passcodes and digital phone evidence. *Id*. at 3-7 (discussing the entanglement between Fifth and Fourth Amendments in investigations of digital devices); *see also United States v. Booker*, 561 F.Supp.3d 924, 939-940 (S.D. Cal. 2021) (while discussing the complexity of *Patane's* application, the Court granted the motion to suppress on voluntariness grounds because information on phone was fruit of a coerced statement). The issue presented in Anderson's case – whether fruits from a digital phone obtained by an *unMirandized* statement are admissible – has been addressed by other courts. In *United States v. Djibo*, the Court declined to apply *Patane* and outlined its reasons. 151 F. Supp. 3d 297, 309-310 (E.D.N.Y. 2015). The Court held:

> The third reason *Patane* should not be applied here is because, as the *Riley* court held, a cell phone is not just a physical object containing information. It is more personal than a purse or a wallet, and certainly more so than the firearm that was used in evidence against Respondent Patane. It is the combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life, and it pinpoints the whereabouts of the owner over time with greater precision than any tool heretofore used by law enforcement without aid of a warrant. In today's modern world, a cell phone passcode is the proverbial "key to a man's kingdom."

Id. at 310; *but see United States v. Hernandez*, No. 18-CR-1888-L, 2018 WL 3862017, at * 4 (S.D. Cal. Aug. 13, 2018)(applying *Patane* and admitting fruits because statement was voluntary). As in *Djibo*, the Court should find *Patane* inapplicable when applied to the admissibility of a digital device.

VI. The inevitable discovery doctrine is inapplicable.

"Evidence discovered through the use of an unlawfully obtained statement is

admissible…'[i]f the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means.'" *United States v. Clark*, No. CR 3:22-30012-MGM, 2023 WL 4706521, at *6 (D. Mass. July 21, 2023). To consider inevitable discovery claims, courts ask "first, whether the legal means by which the evidence would have been discovered was truly independent; second, whether the use of the legal means would have inevitably led to the discovery of the evidence; and third, whether applying the inevitable discovery rule would either provide an incentive for police misconduct or significantly weaken constitutional protections." *Id* at 6. If "demonstrated historical facts shown by a preponderance of the evidence…show that the evidence would have come to light through lawful means," then discovery is inevitable. *Id* at 7.

In claiming that the inevitable discovery doctrine applies, the government relies on two grounds: (1) that the warrant permitted the search of the phone and (2) that law enforcement possessed the technical ability to access the phone's data. *See* ECF Doc. 21 at 8. First, the plain language of the warrant refutes the government's contention that officers possessed legal authority to search the phone's contents, as argued infra, and the government does not indicate that police intended to seek a separate warrant to search the phone. The lack of a legal means to search the phone alone precludes the application of the inevitable discovery doctrine.

Additionally, to show that law enforcement could access the phone's contents without Anderson's passcode, the government must show more than citing to anticipated testimony. *See Clark*, 2023 WL 4706521 at 7 (barring application of the inevitable discovery doctrine where a federal agent "testified that the FBI was not able to independently access the user data on Defendant's cellphone at the time of the search and, more than a year later, still lacked that capability at the time of the [suppression] hearing"). This is unlike *United States v. Stiles*, where

the court upheld the seizure and search of the defendant's phone. No. 1:11-CR-00185-JAW, 2014 WL 5106986 at *7-8 (D. Me. Oct. 10, 2014). There, police executed a search warrant of the defendant's residence, found his phone on his nightstand, viewed its contents, and photographed incriminating text messages. *See id*. at 2. Finding that police had probable cause to believe that the phone contained incriminating evidence and actually received a subsequent warrant to search the phone after viewing its contents, the court concluded that the inevitable discovery doctrine applied. *Id* at 8.

In contrast to *Stiles*, while the Magistrate Judge found probable cause to believe Anderson's phone contained evidence, nothing indicated that law enforcement officers sought a warrant to search the phone after viewing its contents. Cf. *United States v. Silvestri*, 787 F.2d 736,745 (1st Cir. 1986) (holding that "[t]he situation where a warrant is obtained after a warrantless search is somewhat different…[t]he inevitability concerns, i.e., whether a warrant would have issued and whether the search would have uncovered the evidence, are pretty much resolved"). In further dissimilarity to *Stiles*, where police negated any concern that application of the doctrine would have incentivized police misconduct by actually applying for a warrant to search the phone, application of the inevitable discovery doctrine here would prompt officers to search the contents of more phones during the execution of unrelated investigations without applying for a separate, on-point warrant. *See Stiles*, 2014 WL 5106986 at *8. Thus, the court must preclude application of the doctrine and find the contents of Anderson's phone inadmissible.

The Government, through AUSA Charles Rombeau, objects.

WHEREFORE, Tyler Anderson respectfully moves the Court to

(a) schedule an evidentiary hearing on this motion; and

(b) suppress any evidence obtained in violation of his Fourth and Fifth Amendment Rights.

Respectfully submitted,

/s/ Dorothy E. Graham
Dorothy E. Graham
N.H. Bar #11292

CERTIFICATE OF SERVICE

I hereby certify that on the above document was served electronically upon all counsel of record through the CM/ECF filing system on February 27, 2024.

/s/ Dorothy E. Graham
Dorothy E. Graham